UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/042,652	01/08/2002	Jeffrey Bruce Lotspiech	ARC920010090US1	7388

7590 09/26/2008

John L. Rogitz
Rogitz & Associates
750 B Street, Suite 3120
San Diego, CA 92101

EXAMINER	
WYSZYNSKI, AUBREY H	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/042,652	LOTSPIECH ET AL.	
	Examiner	Art Unit	
	AUBREY H. WYSZYNSKI	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3,7,8,12,13,15-22 and 41-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3, 7, 8, 12, 13, 15-22 and 41-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is meant to replace the Office Action sent on 7/31/08 which was sent in error.

2. The response of 3/31/08 was received and considered.

3. Claims 1, 2, 4-6, 9-11, 14, 23-40, 47 and 48 are canceled.

4. Claims 3, 7, 8, 12, 13, 15-22 and 41-46 are pending.

Response to Arguments

5. Applicant's arguments filed 3/31/08 have been fully considered but they are not persuasive.

6. The applicant argues “claims 17-22 had been rejected solely based on obviousness-type double patenting, which rejections were over come by a terminal disclaimer filed previously”. However, the terminal disclaimer filed previously (01/19/2006) by the applicant was disapproved.

7. The applicant has amended claim 1 (now incorporated into claim 17) to overcome the 101 rejection. Therefore the rejections under 35 U.S.C. §101 have been withdrawn.

8. The applicant has amended claims 41-46 to overcome the rejections under §112, 2nd paragraph. Therefore, the rejections have been withdrawn.

9. Applicant argues, “Claims 41-46 have been broadened to remove them from the structures of the sixth paragraph section of 112, rendering all pending claims patentable on the basis of the Board's Decision." However, the Board did not decide claims 41-46

were allowable after overcoming the deficiencies under 112. The Board's Decision recites "As a consequence of the new ground of rejection above, we pro forma reverse the outstanding prior art rejections of claims 41 through 46 as being anticipated by Richards. The subject matter encompassed by the claims on appeal must be reasonably understood without resort to speculation. Presently, speculation and conjecture must be utilized by us and by the artisan inasmuch as the claims on appeal do not adequately reflect what the disclosed invention is. Note In re Steele, 305 F.2d 859, 862 (CCPA 1962) (A prior art rejection cannot be sustained if the hypothetical person of ordinary skill in the art would have to make speculative assumptions concerning the meaning of claim language.); Note also In re Wilson, 424 F.2d 1382, 1385 (CCPA 1970)."

Double Patenting

10. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

11. Claims 3, 7, 8, 12, 13, 15-22 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 14-16 of Lotspiech et al., U.S. Patent No. 7,039,803 (application number 09/770,877) in view of Richards, US 6,690,795 and further in view of Ishiguro, US 2002/0083319.

Please see the rejection below for further clarification.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claim 3, 7, 8, 12, 13, 15-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech, in view of Richards and further in view of Ishiguro

Regarding claim 17, Richards discloses a computer-implemented method for securely transmitting multicast data (fig. 1), comprising: encrypting at least one title T/program A (fig. 2, #2), with at least title key K_T /Segment Key (fig. 2, #2), and encrypting the title key K_T/Segment Key, with at least one channel-unique key

K_{cu}/Customer_code (fig. 2), using at least one encryption function S/DES (col. 6, lines 8-10), to render a multicast data channel encrypted as $S_{Kcu}(K_T)$, $S_{KT}(T)$, (fig. 2, #9).

Richards lacks a channel-unique key that is a result of a combination of a concatenation of the channel key and session key. However, Ishiguro teaches wherein the channel-unique key K_{cu}/e, is the result of a combination of a channel key K_c/e1, and a session key K_s/e2, wherein the combination is a hash function of a concatenation of the channel key K_c/e1, and session key K_s/e2, (¶ [0104]). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of either Richards with the device of Ishiguro. One of ordinary skill in the art would have been motivated to perform such a modification to the device of Richards because Ishiguro teaches combining the channel key/e1, and session key/e2, to form the channel-unique key/e further improves the security of the authentication procedure and the security of transmitted information by preventing an unauthorized user from posing as an authorized user using a desired piece of electronic equipment (¶[0014] & fig. 7).

Richards further discloses wherein the session key K_s/e2, is encrypted with at least a first encryption scheme B^R_{s1}/DES [Ishiguro, ¶ [0079], to render a session key block/sk2' (Ishiguro, ¶ [0105]), providing at least one player with device keys K_d/license key (Ishiguro, fig. 4), to activate the player [Ishiguro, ¶ [0065]), providing the player with the channel key K_c/e1 (Ishiguro, fig. 6), providing the player with the session key block/sk2' (Ishiguro, fig. 6), wherein the player can determine the session key K_s/e2, from the session key block/sk2', using the device keys K_d/license key (Ishiguro, ¶

[0105]), periodically refreshing the channel key K_c/e1, (Ishiguro, fig. 7, steps 48-51) to enforce subscriptions, wherein a new channel key K_c'/e1, is encrypted with at least a second encryption scheme B^R_{s2}/n-bit block encryption (Ishiguro, ¶ [0241]).

Lotspiech discloses assigning each player in a group of players respective private information I_n;

partitioning players not in a revoked set R into disjoint subsets Sjl,...Sjm having associated subset keys Lij,...Lim; and encrypting the session key Ks with the subset keys Li,…,Lim, to render m encrypted versions of the session key Ks (claim 14 of Lotspiech).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lotspiech with the method of Richards in view of Ishiguro in order to render a multicast data channel in order to securely provide each player with data through the use of an encrypted channel, as taught by Richards (figs 1 and 2, col. 6, lines 8-10).

Regarding claim 3, Lotspiech as modified above further discloses the method of claim 17, wherein the combination is a hash function of a concatenation of the channel key K_c/e1, and session key K_s/e2, (Ishiguro, ¶ [0104]).

Regarding claim 7, Lotspiech as modified above further discloses the method of claim 17, wherein at least one of the providing acts is undertaken in a point-to-point communication (Ishiguro, fig. 1).

Regarding claim 8, Lotspiech as modified above further discloses the method of claim 17, wherein at least one of the providing acts is undertaken as part of a broadcast (Ishiguro, ¶ [0105]).

Regarding claim 12, Lotspiech as modified above further discloses the method of claim 17, comprising selectively updating the session key block [Ishiguro, ¶0128].

Regarding claim 13, Lotspiech as modified above further discloses the method of claim 12, comprising updating the session key block/sk2', by encrypting an updated session key/e2, with at least the encryption scheme B^{R}_{s1}/DES (Ishiguro, ¶ [0079]).

Regarding claim 15, Lotspiech as modified above further discloses the method of claim 17, wherein the new channel key K_c'/e1, is sent in a message that is split (Ishiguro, fig. 7, steps 48-51).

Regarding claim 16, Lotspiech as modified above further discloses the method of claim 17, wherein the new channel key K_c'/e1, is refreshed using plural messages (Ishiguro, fig. 7, steps 48-51).

Regarding claims 18-22, Lotspiech discloses these limitations in claims 14-16.

Claim Rejections - 35 USC § 102

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

15. Claims 41-46 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Number 6,690,795 to Richards.

Regarding claim 41 and 43, Richards discloses a computer-implemented player/system, for decrypting streamed content (col. 2, lines 42-44; col. 1, lines 21-23), comprising: at least one device key K_d/UEV (fig. 14), wherein the player decrypting a session key K_s/CAK, using the device key K_d/UEV, wherein the player also decrypts a channel unique key K_{cu}/CCK, using at least the session key K_s/CAK, the player further deriving a title key K_T/PK, using at least the channel unique key K_{cu}/CCK, the title key K_T/PK, being useful for decrypting content (fig. 14).

Regarding claim 42, Richards discloses the player/system, of claim 41, wherein the content is multicast to the player (col. 1, lines 13-18).

Regarding claim 44, Richards discloses a computer program device comprising: a computer program storage device including a program of instructions usable by a computer (col. 2, line 63), to undertake logic comprising: receiving private information I_u

/UEV register (fig. 14) upon registration with a content provider, subscribing to at least one content channel provided by the content provider (col. 3, lines 7-12), receiving at least one encrypted channel key K_c/control channel key (fig. 14), at least partially in response to subscribing to the channel, deriving the channel key K_c/control channel key, using the information I_u/UEV, and using at least the channel key K_c/control channel key, to decrypt content streamed over the channel (fig. 14).

Regarding claim 45, Richards discloses the computer program device of claim 44, the logic further comprising: receiving at least one session key block/DES (col. 21 lines 31-32), deriving at least one session key K_s/segment key, from the session key block using at least one of plural device key K_d/customer code (fig. 8, #58).

Regarding claim 46, Richards discloses the computer program device of claim 45, the logic further comprising: using the session key K_s/segment key, and channel key K_c/control channel key, to derive a channel unique key K_{cu}/channel access key, and using the channel unique key K_{cu}/channel access key, to decrypt a title key K_T/program key, useful for decrypting the content (fig. 27 & 28).

Conclusion

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AUBREY H. WYSZYNSKI whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aubrey H Wyszynski/
Examiner, Art Unit 2134

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2134